

(書誌+要約+請求の範囲)

(19)【発行国】日本国特許庁(JP)
(12)【公報種別】公開特許公報(A)
(11)【公開番号】特開平8-171535
(43)【公開日】平成8年(1996)7月2日
(54)【発明の名称】コンピュータ・データの機密保護方法
(51)【国際特許分類第6版】

G06F 15/00 330 Z 9364-5L

12/14 320 B

C

G09C 1/00 7259-5J

H04L 9/32

【FI】

H04L 9/00 A

【審査請求】未請求

【請求項の数】31

【出願形態】OL

【全頁数】12

(21)【出願番号】特願平6-239003

(22)【出願日】平成6年(1994)10月3日

(31)【優先権主張番号】08/130126

(32)【優先日】1993年10月4日

(33)【優先権主張国】米国(US)

(71)【出願人】

【識別番号】594071860

【氏名又は名称】アディソン・エム・フィッシャー

【住所又は居所】アメリカ合衆国 フロリダ州33942, ネイブルズ, マーチャンタイル・アベニュー
1, 4073番

(72)【発明者】

【氏名】アディソン・エム・フィッシャー

【住所又は居所】アメリカ合衆国 フロリダ州33942, ネイブルズ, マーチャンタイル・アベニュー
1, 4073番

(74)【代理人】

【弁理士】

【氏名又は名称】小笠原 史朗

(57)【要約】(修正有)

【目的】預託された機密情報を持つ管理者が、情報受信の権利を有する関係者以外の人物に情報の漏洩を防ぐ方法と装置の提供。

【構成】コンピュータ購入直後の任意の識別／定義局面と機密情報検索局面を用い、定義局面で、真実の所有者／顧客は、暗号化されたパスワードデータと自己識別データの預託記録を定義する。ユーザが、パスワード、または自分自身を独特に記述する一連の情報を入力後に検索用の他の機密情報を自発的に預託する。識別印は、機密情報(ユーザの暗号化パスワードなど)と結合され、管理者の公開鍵の制御下で暗号化される。独自の識別データを入力後、ユーザは、システムを保護するためのパスワードを選択し、全ての個人識別データは、パスワードと共に、管理者の公開鍵を用いて暗号化され、例えば、ユーザのコンピュータ内に預託機密保護記録として記憶される。パスワードは、ユーザのディスク上の全データの暗号化に用いられる。

【特許請求の範囲】

【請求項1】コンピュータユーザの機密デジタル情報が、後に管理者によって回復できるようにするためのコンピュータ操作方法であって、特定のコンピュータユーザを識別するデジタル識別情報を確立するステップと、識別情報にユーザの機密情報を結合させるステップと、前記結合されたデジタル情報が管理者によってのみ解読可能なように、前記結合されたデジタル情報の少なくとも一部を暗号化するステップと、暗号化されたデジタル情報を管理者による処理用に記憶するステップとを備える、コンピュータ操作方法。

【請求項2】識別情報の少なくとも一部がハッシュ化される、請求項1に記載のコンピュータ操作方法。

【請求項3】識別情報の少なくとも一部が平文で記憶される、請求項1に記載のコンピュータ操作方法。

【請求項4】前記確立ステップは、コンピュータユーザに、複数のユーザ識別特徴データを提供させるステップを含む、請求項1に記載のコンピュータ操作方法。

【請求項5】前記確立ステップは、ユーザが、身体的特徴情報を提供するステップを含む、請求項1に記載のコンピュータ操作方法。

【請求項6】前記確立ステップは、ユーザが、ユーザの公開鍵を提供するステップを含む、請求項1に記載のコンピュータ操作方法。

【請求項7】前記機密情報を回復する試みが為される場合に、管理者が従うべき命令をコンピュータユーザに要求するステップをさらに含む、請求項1に記載のコンピュータ操作方法。

【請求項8】前記確立ステップは、前記機密情報を回復しようと試みる人物に対して、管理者が尋ねるべき少なくとも一つの質問を、ユーザが提供するステップを含む、請求項1に記載のコンピュータ操作方法。

【請求項9】前記暗号化ステップは、暗号化鍵を生成するステップと、前記暗号化鍵を用いて少なくとも前記機密情報を暗号化するステップとを含む、請求項1に記載のコンピュータ操作方法。

【請求項10】前記暗号化ステップは、管理者の公開鍵を用いて前記暗号化鍵を暗号化するステップを含む、請求項9に記載のコンピュータ操作方法。

【請求項11】前記記憶ステップは、コンピュータユーザのメモリ媒体に前記暗号化されたデジタル情報を記憶するステップを含む、請求項1に記載のコンピュータ操作方法。

【請求項12】前記記憶ステップは、管理者を記述する情報を平文で記憶するステップを含む、請求項1に記載のコンピュータ操作方法。

【請求項13】管理者が、預託記録内に含まれる預託されたデジタル機密情報を申込者に安全に与えることができるようとするためのコンピュータ操作方法であって、申込者を識別する信用証明書を取得するステップと、預託された記録を取得するステップと、預託された記録を解読するステップと、申込者の信用証明証を、預託された情報内の識別情報と比較するステップと、信用証明書が預託された識別情報と一致する場合に、申込者に機密情報を与えるステップとを備える、コンピュータ操作方法。

【請求項14】識別情報は、管理者が入手することのできる情報の一部として暗号化される、請求項13に記載のコンピュータ操作方法。

【請求項15】識別情報のハッシュは、管理者が入手することのできる情報の一部として暗号化される、請求項13に記載のコンピュータ操作方法。

【請求項16】前記預託情報が、紙上にデジタルフォームで印刷される、請求項13に記載のコンピュータ操作方法。

【請求項17】識別デジタル情報は、氏名、住所、電話番号、身長、体重、誕生日、容貌、人種、目の色、出生地、会社、役職、事業地、社員証、上司、識別番号、デジタル化された指紋、デジタル化された写真、デジタル化された声見本、デジタル化された網膜情報、ユーザのDNAに関する情報、デジタル化された筆跡見本、デジタル化されたキータイピング、筆法分析、DNAパターン、および一般的にコンピュータユーザ以外には知られていない事実の内の少なくとも一つを含む、請求項13に記載のコンピュータ操作方法。

【請求項18】解読ステップは、前記預託記録の少なくとも一部を解読するために管理者の個人鍵を使用するステップを含む、請求項13に記載のコンピュータ操作方法。

【請求項19】解読ステップは、預託記録を解読するために管理者の個人鍵を使用し、預託記録内の他のフィールドを暗号化するのに用いられるランダム暗号化鍵をアクセスするステップ

を含む、請求項13に記載のコンピュータ操作方法。

【請求項20】預託記録内の複数のフィールドのハッシュを計算するステップをさらに含む、請求項13に記載のコンピュータ操作方法。

【請求項21】信用証明書が預託データに充分に一致しない場合は、申込者に更なる信用証明書を要求するステップをさらに含む、請求項13に記載のコンピュータ操作方法。

【請求項22】前記要求ステップは、申込者に対して預託記録内で規定されている通りに質問をするステップを含む、請求項21に記載のコンピュータ操作方法。

【請求項23】複数の管理者から機密情報の異なる部分を取得するステップをさらに含む、請求項13に記載のコンピュータ操作方法。

【請求項24】識別デジタル情報の少なくとも一部は、前記情報のハッシュによって示される、請求項13に記載のコンピュータ操作方法。

【請求項25】処理装置、および当該処理装置に結合されるメモリ装置を有するコンピュータシステムにおいて、後に管理者がコンピュータユーザの機密デジタル情報を回復できるようにするため前記メモリ装置に記憶されるデジタルデータ構造であって、コンピュータユーザを識別する識別情報を記憶する手段と、暗号化された形で機密デジタル情報を記憶する手段とを備える、デジタルデータ構造。

【請求項26】前記管理者を識別する情報を記憶する手段をさらに含む、請求項25に記載のデジタルデータ構造。

【請求項27】前記機密デジタル情報を暗号化するために用いられる暗号化鍵の暗号化されたバージョンを記憶する手段をさらに含む、請求項25に記載のデジタルデータ構造。

【請求項28】前記識別情報および前記機密デジタル情報のハッシュを記憶する手段をさらに含む、請求項25に記載のデジタルデータ構造。

【請求項29】前記識別情報記憶手段は、氏名、住所、電話番号、身長、体重、誕生日、容貌、人種、目の色、出生地、会社、役職、事業地、社員証、上司、識別番号、デジタル化された指紋、デジタル化された写真、デジタル化された声見本、デジタル化された網膜情報、ユーザのDNAに関する情報、デジタル化された筆跡見本、デジタル化されたキータイピング、筆法分析、DNAパターン、および一般的にコンピュータユーザ以外には知られていない事実の内の少なくとも一つを記憶する手段を含む、請求項25に記載のデジタルデータ構造。

【請求項30】申込者が前記機密情報へのアクセスを得ようとする際に、管理者が従うべき命令を記憶する手段をさらに含む、請求項25に記載のデジタルデータ構造。

【請求項31】管理者が、前記機密情報を回復しようと試みる人物に対して問うべき少なくとも一つの質問を記憶する手段をさらに含む、請求項25に記載のデジタルデータ構造。